SYNCHRONIZATION OF ENCRYPTION IN A WIRELESS COMMUNICATION SYSTEM

ABSTRACT OF THE DISCLOSURE

Disclosed embodiments include a method for synchronizing a cryptosystem. In one embodiment, the method uses existing control data that is transmitted as part of a connection establishment process in a wireless communication system. In one embodiment, messages that are normally sent between a base station and a remote unit during the setup of both originating and terminating calls are parsed to detect a particular control message that indicates the start of telephony data transmission. Detection of this message indicates a point at which encryption/decryption can begin, and is used to synchronize the cryptosystem. Synchronizing a cryptosystem involves generating an RC4 state space in a keyed-autokey ("KEK") encryption system. In one embodiment, Lower Medium Access Channel ("LMAC") messages are used according to a wireless communication protocol. This is convenient because the LMAC messages are passed through the same Associated Control Channel ("ACC") processing that encrypts and decrypts the telephony data.